

Oracle Critical Patch Update Advisory - October 2018

Description

A Critical Patch Update is a collection of patches for multiple security vulnerabilities. Critical Patch Update patches are usually cumulative, but each advisory describes only the security fixes added since the previous Critical Patch Update advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security fixes. Please refer to:

- [Critical Patch Updates, Security Alerts and Bulletins](#) for information about Oracle Security Advisories.

Oracle continues to periodically receive reports of attempts to maliciously exploit vulnerabilities for which Oracle has already released fixes. In some instances, it has been reported that attackers have been successful because targeted customers had failed to apply available Oracle patches. Oracle therefore strongly recommends that customers remain on actively-supported versions and apply Critical Patch Update fixes without delay.

This Critical Patch Update contains 301 new security fixes across the product families listed below. Please note that an MOS note summarizing the content of this Critical Patch Update and other Oracle Software Security Assurance activities is located at [October 2018 Critical Patch Update: Executive Summary and Analysis](#).

Affected Products and Patch Information

Security vulnerabilities addressed by this Critical Patch Update affect the products listed below. The product area is shown in the Patch Availability Document column. Please click on the links in the Patch Availability Document column below to access the documentation for patch availability information and installation instructions.

| Affected Products and Versions | Patch Availability Document |
|--|---|
| Application Management Pack for Oracle E-Business Suite, versions 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 | E-Business Suite |
| Enterprise Manager Base Platform, versions 12.1.0.5, 13.2 | Enterprise Manager |
| Enterprise Manager for MySQL Database, version 13.2 | Enterprise Manager |
| Enterprise Manager Ops Center, versions 12.2.2, 12.3.3 | Enterprise Manager |
| Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers, versions Prior to XCP2352 and Prior to XCP3050 | Systems |
| Hyperion BI+, version 11.1.2.4 | Fusion Middleware |
| Hyperion Common Events, version 11.1.2.4 | Fusion Middleware |
| Hyperion Data Relationship Management, version 11.1.2.4.345 | Fusion Middleware |
| Hyperion Essbase Administration Services, version 11.1.2.4 | Fusion Middleware |
| Instantis EnterpriseTrack, versions 17.1, 17.2, 17.3 | Oracle Construction and Engineering S |
| JD Edwards EnterpriseOne Orchestrator, version 9.2 | JD Edwards |
| JD Edwards EnterpriseOne Tools, version 9.2 | JD Edwards |
| MICROS Lucas, version 2.9.5 | Retail Applications |
| MICROS PC Workstation 2015, versions Prior to BIOS 01.3.0.2i | MICROS PC Workstation |
| MICROS Relate CRM Software, versions 10.8, 11.4 | Retail Applications |
| MICROS Retail-J, versions 12.1.2, 13.0.0 | Retail Applications |
| MICROS XBRI, versions 10.5.0, 10.6.0, 10.7.0, 10.8.1, 10.8.2, 10.8.3 | Retail Applications |
| MySQL Connectors, versions 8.0.12 and prior | MySQL |
| MySQL Enterprise Monitor, versions 3.4.9.4237 and prior, 4.0.6.5281 and prior, 8.0.2.8191 and prior | MySQL |
| MySQL Server, versions 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior, 8.0.12 and prior | MySQL |
| Oracle Adaptive Access Manager, versions 11.1.1.7.0, 11.1.2.3.0 | Fusion Middleware |
| Oracle Agile Engineering Data Management, versions 6.1.3, 6.2.0, 6.2.1 | Oracle Supply Chain Products |
| Oracle Agile PLM, versions 9.3.3, 9.3.4, 9.3.5, 9.3.6 | Oracle Supply Chain Products |
| Oracle Agile Product Lifecycle Management for Process, version 6.2.0.0 | Oracle Supply Chain Products |
| Oracle API Gateway, version 11.1.2.4.0 | Fusion Middleware |
| Oracle Banking Platform, versions 2.5.0, 2.6.0, 2.6.1, 2.6.2 | Oracle Banking Platform |

| Affected Products and Versions | Patch Availability Document |
|--|--|
| Oracle BI Publisher, versions 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 | Fusion Middleware |
| Oracle Big Data Discovery, version 1.6.0 | Fusion Middleware |
| Oracle Business Intelligence Enterprise Edition, versions 11.1.1.7.0, 11.1.1.9.0, 12.2.1.3.0, 12.2.1.4.0 | Fusion Middleware |
| Oracle Communications Application Session Controller, versions Prior to 3.7.1M0 | Oracle Communications Application Session Controller |
| Oracle Communications Instant Messaging Server, versions prior to 10.0.1 | Oracle Communications Instant Messaging Server |
| Oracle Communications Messaging Server, versions prior to 8.0.2 | Oracle Communications Convergence |
| Oracle Communications MetaSolv Solution, version 6.3.0 | Oracle Communications MetaSolv Solu |
| Oracle Communications Performance Intelligence Center (PIC) Software, versions prior to 10.2.1 | Oracle Communications Performance Intelligence Center (PIC) Software |
| Oracle Communications User Data Repository, versions prior to 12.2.0 | Oracle Communications User Data Repository |
| Oracle Configuration Manager, versions 12.1.2.0.2, 12.1.2.0.5 | Enterprise Manager |
| Oracle Database Server, versions 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c | Database |
| Oracle Demantra Demand Management, versions 7.3.5, 12.2 | Oracle Supply Chain Products |
| Oracle Directory Server Enterprise Edition, version 11.1.1.7 | Fusion Middleware |
| Oracle E-Business Suite, versions 12.1.1, 12.1.2, 12.1.3, 12.2.3, 12.2.4, 12.2.5, 12.2.6, 12.2.7 | E-Business Suite |
| Oracle Endeca Information Discovery Integrator, versions 3.1.0, 3.2.0 | Fusion Middleware |
| Oracle Endeca Information Discovery Studio, versions 3.1.0, 3.2.0 | Fusion Middleware |
| Oracle Endeca Server, versions 7.6.1, 7.7.0 | Fusion Middleware |
| Oracle Enterprise Repository, versions 11.1.1.7.0, 12.1.3.0.0 | Fusion Middleware |
| Oracle Fusion Middleware MapViewer, versions 12.1.3.0, 12.2.1.3 | Fusion Middleware |
| Oracle GlassFish Server, version 3.1.2 | Fusion Middleware |
| Oracle GoldenGate, versions 12.1.2.1.0, 12.2.0.2.0, 12.3.0.1.0 | Oracle GoldenGate |
| Oracle GoldenGate for Big Data, versions 12.2.0.1, 12.3.1.1, 12.3.2.1 | Fusion Middleware |
| Oracle Healthcare Translational Research, version 3.1.0 | Health Sciences |

| Affected Products and Versions | Patch Availability Document |
|--|--|
| Oracle Hospitality Cruise Fleet Management, version 9.0 | Oracle Hospitality Cruise Fleet Management |
| Oracle Hospitality Cruise Shipboard Property Management System, version 8.0 | Oracle Hospitality Cruise Shipboard Property Management System |
| Oracle Hospitality Gift and Loyalty, version 9.0, 9.1 | Oracle Hospitality Gift and Loyalty |
| Oracle Hospitality Guest Access, versions 4.2.0, 4.2.1 | Oracle Hospitality Guest Access |
| Oracle Hospitality Materials Control, version 18.1 | Oracle Hospitality Materials Control |
| Oracle Hospitality Reporting and Analytics, version 9.0, 9.1 | Oracle Hospitality Reporting and Analy |
| Oracle HTTP Server, version 12.2.1.3 | Fusion Middleware |
| Oracle Identity Analytics, version 11.1.1.5.8 | Fusion Middleware |
| Oracle Identity Management Suite, versions 11.1.2.3.0, 12.2.1.3.0 | Fusion Middleware |
| Oracle Identity Manager, versions 11.1.2.3.0, 12.2.1.3.0 | Fusion Middleware |
| Oracle iLearning, versions 6.1, 6.2 | iLearning |
| Oracle Insurance Calculation Engine, versions 10.1.1, 10.2.1 | Oracle Insurance Applications |
| Oracle Insurance Rules Palette, versions 10.0, 10.1, 10.2, 11.0, 11.1 | Oracle Insurance Applications |
| Oracle Java SE, versions 6u201, 7u191, 8u181, 11 | Java SE |
| Oracle Java SE Embedded, version 8u181 | Java SE |
| Oracle JRockit, version R28.3.19 | Java SE |
| Oracle Outside In Technology, versions 8.5.3, 8.5.4 | Fusion Middleware |
| Oracle Real-Time Decision Server, version 3.2.1 | Fusion Middleware |
| Oracle Retail Allocation, versions 15.0, 16.0 | Retail Applications |
| Oracle Retail Assortment Planning, versions 14.1, 15.0, 16.0 | Retail Applications |
| Oracle Retail Back Office, versions 13.3, 13.4, 14, 14.1 | Retail Applications |
| Oracle Retail Central Office, version 14.1 | Retail Applications |
| Oracle Retail Customer Management and Segmentation Foundation, versions 16.0, 17.0 | Retail Applications |
| Oracle Retail Extract Transform and Load, versions 13.0, 13.1, 13.2 | Retail Applications |
| Oracle Retail Financial Integration, versions 13.2, 14.0, 14.1, 15.0, 16.0 | Retail Applications |
| Oracle Retail Integration Bus, version 14.1.2 | Retail Applications |
| Oracle Retail Invoice Matching, versions 15.0, 16.0 | Retail Applications |

| Affected Products and Versions | Patch Availability Document |
|--|---------------------------------------|
| Oracle Retail Open Commerce Platform, versions 5.3, 6.0, 6.0.1 | Retail Applications |
| Oracle Retail Order Broker, versions 5.0, 5.1, 5.2, 15.0, 16.0 | Retail Applications |
| Oracle Retail Point-of-Service, versions 13.4, 14.0, 14.1 | Retail Applications |
| Oracle Retail Predictive Application Server, versions 14.0, 14.1, 15.0, 16.0 | Retail Applications |
| Oracle Retail Returns Management, version 14.1 | Retail Applications |
| Oracle Retail Sales Audit, versions 15.0, 16.0 | Retail Applications |
| Oracle Retail Xstore Point of Service, versions 6.5.12, 7.0.7, 7.1.7, 15.0.2, 16.0.4, 17.0.2 | Retail Applications |
| Oracle Service Bus, versions 12.1.3.0.0, 12.2.1.3.0 | Fusion Middleware |
| Oracle Transportation Management, version 6.3.7 | Oracle Supply Chain Products |
| Oracle Tuxedo, version 12.1.1.0 | Fusion Middleware |
| Oracle Virtual Directory, versions 11.1.1.7.0, 11.1.1.9.0 | Fusion Middleware |
| Oracle VM VirtualBox, versions prior to 5.2.20 | Virtualization |
| Oracle WebCenter Portal, versions 11.1.1.9.0, 12.2.1.3.0 | Fusion Middleware |
| Oracle WebCenter Sites, versions 11.1.1.8.0, 12.2.1.3.0 | Fusion Middleware |
| Oracle WebLogic Server, versions 10.3.6.0, 12.1.3.0, 12.2.1.3, prior to Docker 12.2.1.3.20180913 | Fusion Middleware |
| OSS Support Tools, versions prior to 18.4 | Support Tools |
| PeopleSoft Enterprise Interaction Hub, version 9.1.0.0 | PeopleSoft |
| PeopleSoft Enterprise PeopleTools, versions 8.55, 8.56, 8.57 | PeopleSoft |
| Primavera Gateway, versions 15.2, 16.2, 17.12 | Oracle Construction and Engineering S |
| Primavera P6 Enterprise Project Portfolio Management, versions 8.4, 15.1, 15.2, 16.1, 16.2, 18.8, 17.7 - 17.12 | Oracle Construction and Engineering S |
| Primavera Unifier, versions 15.1, 15.2, 16.1, 16.2, 17.1-17.12, 18.1-18.8 | Oracle Construction and Engineering S |
| Siebel Applications, versions 18.7, 18.8, 18.9 | Siebel |
| Solaris, versions 10, 11.3, 11.4 | Systems |
| SPARC Enterprise M3000, M4000, M5000, M8000, M9000 Servers, versions prior to XCP 1123 | Systems |
| Spatial, versions 2.0, 2.1, 2.2 | Oracle Big Data Graph |

Note:

- Vulnerabilities affecting Oracle Database and Oracle Fusion Middleware may affect Oracle Fusion Applications, so Oracle customers should refer to Oracle Fusion Applications Critical Patch Update Knowledge Document, [My Oracle Support Note 1967316.1](#) for information on patches to be applied to Fusion Application environments.
- Vulnerabilities affecting Oracle Solaris may affect Oracle ZFSSA so Oracle customers should refer to the Oracle and Sun Systems Product Suite Critical Patch Update Knowledge Document, [My Oracle Support Note 2160904.1](#) for information on minimum revisions of security fixes required to resolve ZFSSA issues published in Critical Patch Updates and Solaris Third Party bulletins.
- Users running Java SE with a browser can download the latest release from <http://java.com>. Users on the Windows and Mac OS X platforms can also use [automatic updates](#) to get the latest release.

Risk Matrix Content

Risk matrices list only security vulnerabilities that are newly fixed by the patches associated with this advisory. Risk matrices for previous security fixes can be found in [previous Critical Patch Update advisories](#). An English text version of the risk matrices provided in this document is [here](#).

Several vulnerabilities addressed in this Critical Patch Update affect multiple products. Each vulnerability is identified by a **CVE#** which is a unique identifier for a vulnerability. A vulnerability that affects multiple products will appear with the same CVE# in all risk matrices. A CVE# shown in *italics* indicates that this vulnerability impacts a different product, but also has impact on the product where the italicized CVE# is listed.

Security vulnerabilities are scored using CVSS version 3.0 (see [Oracle CVSS Scoring](#) for an explanation of how Oracle applies CVSS version 3.0).

Oracle conducts an analysis of each security vulnerability addressed by a Critical Patch Update. Oracle does not disclose detailed information about this security analysis to customers, but the resulting Risk Matrix and associated documentation provide information about the type of vulnerability, the conditions required to exploit it, and the potential impact of a successful exploit. Oracle provides this information, in part, so that customers may conduct their own risk analysis based on the particulars of their product usage. For more information, see [Oracle vulnerability disclosure policies](#).

The protocol in the risk matrix implies that all of its secure variants (if applicable) are affected as well. For example, if HTTP is listed as an affected protocol, it implies that HTTPS (if applicable) is also affected. The secure variant of a protocol is listed in the risk matrix only if it is the *only* variant affected, e.g. HTTPS will typically be listed for vulnerabilities in SSL and TLS.

Workarounds

Due to the threat posed by a successful attack, Oracle strongly recommends that customers apply Critical Patch Update fixes as soon as possible. Until you apply the Critical Patch Update fixes, it may be possible to reduce the risk of successful attack by blocking network protocols required by an attack. For attacks that require certain privileges or access to certain packages, removing the privileges or the ability to access the packages from users that do not need the privileges may help reduce the risk of successful attack. Both approaches may break application functionality, so Oracle strongly recommends that customers test changes on non-production systems. Neither approach should be considered a long-term solution as neither corrects the underlying problem.

Skipped Critical Patch Updates

Oracle strongly recommends that customers apply security fixes as soon as possible. For customers that have skipped one or more Critical Patch Updates and are concerned about products that do not have security fixes announced in this Critical Patch Update, please review [previous Critical Patch Update advisories](#) to determine appropriate actions.

Critical Patch Update Supported Products and Versions

Patches released through the Critical Patch Update program are provided only for product versions that are covered under the Premier Support or Extended Support phases of the [Lifetime Support Policy](#). Oracle recommends that customers plan product upgrades to ensure that patches released through the Critical Patch Update program are available for the versions they are currently running.

Product releases that are not under Premier Support or Extended Support are not tested for the presence of vulnerabilities addressed by this Critical Patch Update. However, it is likely that earlier versions of affected releases are also affected by these vulnerabilities. As a result, Oracle recommends that customers upgrade to supported versions.

Database, Fusion Middleware, and Oracle Enterprise Manager products are patched in accordance with the Software Error Correction Support Policy explained in [My Oracle Support Note 209768.1](#). Please review the [Technical Support Policies](#) for further guidelines regarding support policies and phases of support.

Credit Statement

The following people or organizations reported security vulnerabilities addressed by this Critical Patch Update to Oracle:

- 360 A-TEAM: CVE-2018-3245

- Add of MeePwn working with Trend Micro's Zero Day Initiative: CVE-2018-2909, CVE-2018-3290, CVE-2018-3296, CVE-2018-3297
- Andrej Simko of Accenture: CVE-2018-3242, CVE-2018-3243
- Andrej Simko of Accenture working with iDefense Labs: CVE-2018-3256
- Anonymous researcher working with Trend Micro's Zero Day Initiative: CVE-2018-3291, CVE-2018-3292, CVE-2018-3298
- Artem Smotrakov: CVE-2018-3139
- Aurelien Salomon of Pure Hacking: CVE-2018-3204
- Badcode of Knownsec 404 Team: CVE-2018-3245, CVE-2018-3250
- Behzad Najjarpour Jabbari, Secunia Research at Flexera Software: CVE-2018-18223, CVE-2018-18224, CVE-2018-3217, CVE-2018-3218, CVE-2018-3219, CVE-2018-3220, CVE-2018-3221, CVE-2018-3222, CVE-2018-3223, CVE-2018-3224, CVE-2018-3225, CVE-2018-3226, CVE-2018-3227, CVE-2018-3228, CVE-2018-3229, CVE-2018-3230, CVE-2018-3231, CVE-2018-3232, CVE-2018-3233, CVE-2018-3234, CVE-2018-3302
- Devin Rosenbauer of Identity Works LLC: CVE-2018-3179
- Felix Dörre: CVE-2018-3180
- Giulio Comi of Horizon Security: CVE-2018-3205, CVE-2018-3206, CVE-2018-3207
- Graham Steel of Cryptosense: CVE-2018-3210
- Gregory Smiley of Security Compass: CVE-2018-3181
- Hans-Martin Münch: CVE-2018-3168
- Hasan Alqawzai: CVE-2018-3184
- Huy Ngo of Viettel Cyber Security: CVE-2018-3295
- Hysterical Raisins working with Trend Micro's Zero Day Initiative: CVE-2018-2909, CVE-2018-3287, CVE-2018-3296, CVE-2018-3297, CVE-2018-3298
- HzH4k: CVE-2018-3245
- Independent security researcher via Beyond Security's SecuriTeam Secure Disclosure program: CVE-2018-3294
- Jacob Baines of Tenable, Inc.: CVE-2018-2912, CVE-2018-2913, CVE-2018-2914
- Jakub Palaczynski: CVE-2018-3262
- Jason Lang of TrustedSec: CVE-2018-3253
- Jayson Grace of Sandia National Laboratories: CVE-2018-3235, CVE-2018-3236, CVE-2018-3237
- Jim LaValley, Towerwall, Inc.: CVE-2018-3241, CVE-2018-3281
- Jimi Sebree of Tenable, Inc.: CVE-2018-3213
- John Moss of IRM Security: CVE-2018-3167

- Jon King of OPNAV N1, US Navy: CVE-2018-3192
- Jonas Mattsson: CVE-2018-3238
- Kamlapati Choubey of Trend Micro's Zero Day Initiative: CVE-2018-3147
- Koustav Sadhukhan: CVE-2018-2909, CVE-2018-3293, CVE-2018-3295, CVE-2018-3296, CVE-2018-3297, CVE-2018-3298
- Krzysztof Szafranski: CVE-2018-3183
- Li Qiang of the Qihoo 360 Gear Team: CVE-2018-3289, CVE-2018-3290, CVE-2018-3293, CVE-2018-3295
- Li Zhengdong of Hitax: CVE-2018-3191
- Liam Glanfield of IRM Security: CVE-2018-3167
- Liao Xinxi of NSFOCUS Security Team: CVE-2018-3245
- Lilei of Venustech ADLab: CVE-2018-3245
- Lokesh Sharma: CVE-2018-3138
- loopx9: CVE-2018-3191
- Lukasz Mikula: CVE-2018-3132, CVE-2018-3254
- Lukasz Plonka of ING Services Polska: CVE-2018-3208
- Maciej Grabiec: CVE-2018-3140, CVE-2018-3141, CVE-2018-3142
- Marcin Wołoszyn of ING Services Polska: CVE-2018-3175, CVE-2018-3176, CVE-2018-3177, CVE-2018-3178
- Mark Earnest of Identity Works LLC: CVE-2018-3179
- Matthias Kaiser of Code White: CVE-2018-3191, CVE-2018-3197, CVE-2018-3201
- Mauricio Correa of Xlabs: CVE-2018-3172
- Michael Orlitzky: CVE-2018-3174
- Nelson William Gamazo Sanchez of Trend Micro's Zero Day Initiative: CVE-2018-3211
- Or Hanuka of Motorola Solutions: CVE-2018-3127
- Pawel Gocyla: CVE-2018-2902
- Ph0rse of Qihoo 360 Group Okee Team: CVE-2018-3245
- Quang Nguyen of Viettel Cyber Security: CVE-2018-3295
- Root Object working with Trend Micro's Zero Day Initiative: CVE-2018-3288, CVE-2018-3289, CVE-2018-3293
- Sean Metcalf of Trimarc Security: CVE-2018-3253
- Tobias Ospelt of modzero: CVE-2018-3214
- Tom Tervoort of Secura: CVE-2018-2911

- Tzachy Horesh of Motorola Solutions: CVE-2018-3127
- Vahagn Vardanyan: CVE-2018-3215
- WenHui Wang: CVE-2018-3245, CVE-2018-3249
- Xiao Pingge: CVE-2018-3246
- Zhiyi Zhang of 360 ESG Codesafe Team: CVE-2018-3245, CVE-2018-3248, CVE-2018-3249, CVE-2018-3252

Security-In-Depth Contributors

Oracle acknowledges people who have contributed to our Security-In-Depth program (see [FAQ](#)). People are acknowledged for Security-In-Depth contributions if they provide information, observations or suggestions pertaining to security vulnerability issues that result in significant modification of Oracle code or documentation in future releases, but are not of such a critical nature that they are distributed in Critical Patch Updates.

In this Critical Patch Update Advisory, Oracle recognizes the following for contributions to Oracle's Security-In-Depth program.:

- Antonio Sanso
- Cyril Vallicari of ZIWIT/HTTPCS
- Gregory Smiley of Security Compass
- Martin Buchholz of Google
- Mingxuan Song of CNCERT
- Sarath Nair

On-Line Presence Security Contributors

Oracle acknowledges people who have contributed to our On-Line Presence Security program (see [FAQ](#)). People are acknowledged for contributions relating to Oracle's on-line presence if they provide information, observations or suggestions pertaining to security-related issues that result in significant modification to Oracle's on-line external-facing systems.

For this quarter, Oracle recognizes the following for contributions to Oracle's On-Line Presence Security program:

- Alexander Kornbrust of Red Database Security
- Hemanth Joseph of hemanthjoseph.com
- Joby John
- Jose Domingo Carrillo

- Kranthi Kumar
- Mayank of Birla Institute of Technology, Mesra
- Mohammed Fayadh
- Pethuraj M (mr7)
- Pranshu Tiwari
- Rajat Sharma
- Richard Alvariez
- Samet Sahin
- Sébastien Kaul
- Zach Edwards of victorymedium.com
- Zekvan Arslan

Critical Patch Update Schedule

Critical Patch Updates are released on the Tuesday closest to the 17th day of January, April, July and October. The next four dates are:

- 15 January 2019
- 16 April 2019
- 16 July 2019
- 15 October 2019

References

- [Oracle Critical Patch Updates, Security Alerts and Bulletins](#)
- [Critical Patch Update - October 2018 Documentation Map](#)
- [Oracle Critical Patch Updates and Security Alerts - Frequently Asked Questions](#)
- [Risk Matrix Definitions](#)
- [Use of Common Vulnerability Scoring System \(CVSS\) by Oracle](#)
- [English text version of the risk matrices](#)
- [CVRF XML version of the risk matrices](#)
- [Map of CVE to Advisory](#)
- [Software Error Correction Support Policy](#)

Modification History

| Date | Note |
|------------------|--|
| 2018-October-16 | Rev 1. Initial Release. |
| 2018-October-17 | Rev 2. Updated Oracle Java SE Risk Matrix. |
| 2018-October-18 | Rev 3. Updated affected versions of CVE-2018-3128 and CVE-2018-3131 in Oracle Food and Beverage Applications Risk Matrix |
| 2018-October-19 | Rev 4. Updated CVSS score of CVE-2018-3253 and credit statement. |
| 2018-October-30 | Rev 5. Updated credit statement. |
| 2018-December-18 | Rev 6. Updated affected versions for Oracle Outside In Technology vulnerabilities. |

Oracle Database Server Risk Matrix

This Critical Patch Update contains 7 new security fixes for the Oracle Database Server divided as follows:

- 3 new security fixes for the Oracle Database Server. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these fixes are applicable to client-only installations, i.e., installations that do not have the Oracle Database Server installed. The English text form of this Risk Matrix can be found [here](#).
- 1 new security fix for Oracle Big Data Graph. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).
- 3 new security fixes for Oracle GoldenGate. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Component | Package and/or Privilege Required | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK | | | | |
|----------------------|-------------|-----------------------------------|----------|-------------------------------|-----------------------|---------------|----------------|-------------|----|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd | Ir |
| CVE-2018-3259 | Java VM | None | Multiple | Yes | 9.8 | Network | Low | None | |
| CVE-2018-3299 | Oracle Text | None | Multiple | Yes | 8.2 | Network | Low | None | Re |

| CVE# | Component | Package and/or Privilege Required | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK | | | | |
|----------------------|-------------------------|-----------------------------------|----------|-------------------------------|-----------------------|------------------|----------------|-------------|--------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd | Impact |
| CVE-2018-7489 | Rapid Home Provisioning | RHP User | HTTP | No | 2.3 | Adjacent Network | High | Low | Re |

Additional CVEs addressed are below:

- The fix for CVE-2018-7489 also addresses CVE-2017-15095.

Oracle Big Data Graph Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Big Data Graph. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK (s | | | | |
|----------------------|---------|--------------------------------|----------|-------------------------------|--------------------------|---------------|----------------|-------------|-----|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd | U |
| CVE-2016-6814 | Spatial | Big Data Graph (Apache Groovy) | HTTP | Yes | 9.6 | Network | Low | None | Rec |

Oracle GoldenGate Risk Matrix

This Critical Patch Update contains 3 new security fixes for Oracle GoldenGate. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISI | | | | |
|----------------------|-------------------|--------------------|----------|-------------------------------|-----------------------|---------------|----------------|-------------|---|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd | I |
| CVE-2018-2913 | Oracle GoldenGate | Monitoring Manager | TCP | Yes | 10.0 | Network | Low | None | |
| CVE-2018-2912 | Oracle GoldenGate | Manager | TCP | Yes | 7.5 | Network | Low | None | |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RIS | | | |
|----------------------|-------------------|-----------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-2914 | Oracle GoldenGate | Manager | TCP | Yes | 7.5 | Network | Low | None |

Notes:

1. For Linux and Windows platforms, the CVSS score is 9.0 with Access Complexity as High. For all other platforms, the cvss score is 10.0.

Oracle Communications Applications Risk Matrix

This Critical Patch Update contains 14 new security fixes for Oracle Communications Applications. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3 | | | |
|----------------------|--|---------------------------------------|----------|-------------------------------|----------------|---------------|----------------|---|
| | | | | | Base Score | Attack Vector | Attack Complex | F |
| CVE-2015-0235 | Oracle Communications Application Session Controller | Security (Glibc) | Multiple | Yes | 9.8 | Network | Low | I |
| CVE-2017-5645 | Oracle Communications Messaging Server | Convergence (Apache Log4J) | HTTP | Yes | 9.8 | Network | Low | I |
| CVE-2016-0729 | Oracle Communications User Data Repository | Security (Apache Xerces) | HTTP | Yes | 9.8 | Network | Low | I |
| CVE-2015-7501 | Oracle Communications Application Session Controller | Security (Apache Commons Collections) | HTTP | No | 8.8 | Network | Low | |
| CVE-2015-7501 | Oracle Communications Performance | Security (Apache | HTTP | No | 8.8 | Network | Low | |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3 | | | F |
|-----------------------|--|--|----------|-------------------------------|----------------|---------------|----------------|---|
| | | | | | Base Score | Attack Vector | Attack Complex | |
| | Intelligence Center (PIC) Software | Commons Collections) | | | | | | |
| CVE-2016-0635 | Oracle Communications Performance Intelligence Center (PIC) Software | Security (Spring Framework) | HTTP | No | 8.8 | Network | Low | |
| CVE-2016-1182 | Oracle Communications Performance Intelligence Center (PIC) Software | Security (Apache Struts 1) | HTTP | Yes | 8.2 | Network | Low | I |
| CVE-2017-15095 | Oracle Communications Instant Messaging Server | Security (jackson-databind) | HTTP | Yes | 8.1 | Network | High | I |
| CVE-2018-8013 | Oracle Communications MetaSolv Solution | Print preview, Gateway Events (Apache Batik) | HTTP | Yes | 7.3 | Network | Low | I |
| CVE-2016-5080 | Oracle Communications Performance Intelligence Center (PIC) Software | Security (Objective System ASN1C) | Multiple | No | 7.2 | Network | Low | |
| CVE-2016-5019 | Oracle Communications Performance Intelligence Center (PIC) Software | Security (Apache Trinidad) | HTTP | No | 6.7 | Network | Low | |
| CVE-2016-2107 | Oracle Communications Application | Security (OpenSSL) | TLS | Yes | 5.9 | Network | High | I |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | Priority |
|----------------------|--|---------------------------|----------|-------------------------------|------------------|---------------|-------------------|----------|
| | | | | | Base Score | Attack Vector | Attack Complexity | |
| | Session Controller | | | | | | | |
| CVE-2017-3736 | Oracle Communications Performance Intelligence Center (PIC) Software | Security (OpenSSL) | TLS | Yes | 5.9 | Network | High | Low |
| CVE-2014-3490 | Oracle Communications Performance Intelligence Center (PIC) Software | Security (resteasy-jaxrs) | HTTP | Yes | 5.3 | Network | Low | Low |

Additional CVEs addressed are below:

- The fix for CVE-2015-0235 also addresses CVE-2014-7817.
- The fix for CVE-2016-0729 also addresses CVE-2015-0252.
- The fix for CVE-2016-1182 also addresses CVE-2012-1007, CVE-2014-0014 and CVE-2016-1181.
- The fix for CVE-2017-15095 also addresses CVE-2017-7525.
- The fix for CVE-2017-3736 also addresses CVE-2017-3735.

Oracle Construction and Engineering Suite Risk Matrix

This Critical Patch Update contains 10 new security fixes for the Oracle Construction and Engineering Suite. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | Priority |
|----------------------|-------------------|-------------------------------|----------|-------------------------------|------------------|---------------|-------------------|----------|
| | | | | | Base Score | Attack Vector | Attack Complexity | |
| CVE-2018-1275 | Primavera Gateway | Web Access (Spring Framework) | HTTP | Yes | 9.8 | Network | Low | No |
| CVE-2018-7489 | Primavera Gateway | Web Access (jackson-) | HTTP | Yes | 9.8 | Network | Low | No |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|-----------------------|--|-------------------------------|----------|-------------------------------|------------------|---------------|----------------|--------|
| | | | | | Base Score | Attack Vector | Attack Complex | Pri Re |
| | | databind) | | | | | | |
| CVE-2018-12023 | Primavera Unifier | Core (jackson-databind) | HTTP | Yes | 8.1 | Network | High | No |
| CVE-2018-8013 | Instantis EnterpriseTrack | Generic (Apache Batik) | HTTP | Yes | 7.3 | Network | Low | No |
| CVE-2018-1305 | Instantis EnterpriseTrack | Generic (Apache Tomcat) | HTTP | No | 6.5 | Network | Low | Lc |
| CVE-2015-9251 | Primavera Gateway | Admin (jQuery) | HTTP | Yes | 6.1 | Network | Low | No |
| CVE-2018-3241 | Primavera P6 Enterprise Project Portfolio Management | Web Access | HTTP | Yes | 6.1 | Network | Low | No |
| CVE-2018-3281 | Primavera P6 Enterprise Project Portfolio Management | Web Access | HTTP | Yes | 6.1 | Network | Low | No |
| CVE-2018-3148 | Primavera Unifier | Web Access | HTTP | Yes | 6.1 | Network | Low | No |
| CVE-2018-11039 | Primavera P6 Enterprise Project Portfolio Management | Web Access (Spring Framework) | HTTP | Yes | 5.9 | Network | High | No |

Additional CVEs addressed are below:

- The fix for CVE-2018-1275 also addresses CVE-2018-1258.
- The fix for CVE-2018-7489 also addresses CVE-2017-15095 and CVE-2018-12023.

Oracle E-Business Suite Risk Matrix

This Critical Patch Update contains 16 new security fixes for the Oracle E-Business Suite. 14 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

Oracle E-Business Suite products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle E-Business Suite products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security fixes are not listed in the Oracle E-Business Suite risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle E-Business Suite products, Oracle recommends that customers apply the October 2018 Critical Patch Update to the Oracle Database and Oracle Fusion Middleware components of Oracle E-Business Suite. For information on what patches need to be applied to your environments, refer to Oracle E-Business Suite Release 12 Critical Patch Update Knowledge Document (October 2018), [My Oracle Support Note 2445688.1](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|----------------------|-------------------------------------|---------------------------|----------|-------------------------------|------------------|---------------|----------------|----------|
| | | | | | Base Score | Attack Vector | Attack Complex | Priv Rec |
| CVE-2018-3138 | Oracle Application Object Library | Attachments / File Upload | HTTP | Yes | 8.2 | Network | Low | No |
| CVE-2018-3243 | Oracle Applications Framework | None | HTTP | Yes | 8.2 | Network | Low | No |
| CVE-2018-3235 | Oracle Applications Manager | None | HTTP | Yes | 8.2 | Network | Low | No |
| CVE-2018-3189 | Oracle Customer Interaction History | Outcome-Result | HTTP | Yes | 8.2 | Network | Low | No |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|----------------------|--------------------------------|--------------------------------|----------|-------------------------------|------------------|---------------|----------------|----------|
| | | | | | Base Score | Attack Vector | Attack Complex | Priv Rec |
| CVE-2018-3190 | Oracle E-Business Intelligence | Overview Page/Report Rendering | HTTP | Yes | 8.2 | Network | Low | No |
| CVE-2018-3188 | Oracle iStore | Web interface | HTTP | Yes | 8.2 | Network | Low | No |
| CVE-2018-3242 | Oracle Marketing | Marketing Administration | HTTP | Yes | 8.2 | Network | Low | No |
| CVE-2018-3196 | Oracle Partner Management | Partner Dashboard | HTTP | Yes | 8.2 | Network | Low | No |
| CVE-2018-3011 | Oracle Trade Management | User Interface | HTTP | Yes | 8.2 | Network | Low | No |
| CVE-2018-3151 | Oracle iProcurement | E-Content Manager Catalog | HTTP | Yes | 7.5 | Network | Low | No |
| CVE-2018-3236 | Oracle User Management | Reports | HTTP | No | 6.5 | Network | Low | High |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|----------------------|---|---------------------------|----------|-------------------------------|------------------|---------------|----------------|----------|
| | | | | | Base Score | Attack Vector | Attack Complex | Priv Rec |
| | | | | | | | | |
| CVE-2018-3167 | Application Management Pack for Oracle E-Business Suite | User Monitoring | HTTP | Yes | 5.3 | Network | Low | No |
| CVE-2018-3244 | Oracle Application Object Library | Attachments / File Upload | HTTP | Yes | 5.3 | Network | Low | No |
| CVE-2018-3237 | Oracle Applications Manager | Support Cart | HTTP | Yes | 5.3 | Network | Low | No |
| CVE-2018-3256 | Oracle Email Center | Message Display | HTTP | Yes | 4.7 | Network | Low | No |
| CVE-2018-2971 | Oracle Applications Framework | REST Services | HTTP | No | 4.3 | Network | Low | Lo |

Oracle Enterprise Manager Products Suite Risk Matrix

This Critical Patch Update contains 4 new security fixes for the Oracle Enterprise Manager Products Suite. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. None of these fixes are applicable to client-only installations, i.e., installations that do not have the Oracle Enterprise Manager Products Suite installed. The English text form of this Risk Matrix can be found [here](#).

Oracle Enterprise Manager products include Oracle Database and Oracle Fusion Middleware components that are affected by the vulnerabilities listed in the Oracle Database and Oracle Fusion Middleware sections. The exposure of Oracle Enterprise Manager products is dependent on the Oracle Database and Oracle Fusion Middleware versions being used. Oracle Database and Oracle Fusion Middleware security fixes are not listed in the Oracle Enterprise Manager risk matrix. However, since vulnerabilities affecting Oracle Database and Oracle Fusion Middleware versions may affect Oracle Enterprise Manager products, Oracle recommends that customers apply the October 2018 Critical Patch Update to the Oracle Database and Oracle Fusion Middleware components of Enterprise Manager. For information on what patches need to be applied to your environments, refer to Critical Patch Update October 2018 Patch Availability Document for Oracle Products, [My Oracle Support Note 24334771](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 F | | | |
|----------------------|---------------------------------------|---|----------|-------------------------------|--------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs Req'd |
| CVE-2016-4000 | Enterprise Manager Ops Center | Networking (Jython) | HTTP | Yes | 9.8 | Network | Low | None |
| CVE-2017-5645 | Oracle Configuration Manager | Collector of Config and Diag (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low | None |
| CVE-2018-1258 | Enterprise Manager for MySQL Database | EM Plugin: General (Spring Framework) | HTTP | No | 8.8 | Network | Low | Low |
| CVE-2018-0739 | Enterprise Manager Base Platform | Discovery Framework (OpenSSL) | HTTP | Yes | 6.5 | Network | Low | None |

Additional CVEs addressed are below:

- The fix for CVE-2018-0739 also addresses CVE-2017-3738 and CVE-2018-0733.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.

Oracle Financial Services Applications Risk Matrix

This Critical Patch Update contains 2 new security fixes for Oracle Financial Services Applications. Both of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK | | | |
|-----------------------|-------------------------|-----------------------------------|----------|-------------------------------|-----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-12023 | Oracle Banking Platform | Infrastructure (jackson-databind) | HTTP | Yes | 8.1 | Network | High | None |
| CVE-2015-9251 | Oracle Banking Platform | UI (jQuery) | HTTP | Yes | 6.1 | Network | Low | None |

Additional CVEs addressed are below:

- The fix for CVE-2018-12023 also addresses CVE-2018-11307 and CVE-2018-12022.

Oracle Food and Beverage Applications Risk Matrix

This Critical Patch Update contains 4 new security fixes for Oracle Food and Beverage Applications. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Component | Package and/or Privilege Required | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK | | |
|----------------------|--|-----------------------------------|----------|-------------------------------|-----------------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2018-3128 | Oracle Hospitality Reporting and Analytics | Report | HTTP | No | 8.1 | Network | Low |
| CVE-2018-3131 | Oracle Hospitality Gift and Loyalty | Report | None | No | 6.1 | Local | Low |
| CVE-2015-9251 | Oracle Hospitality Materials Control | MobileAuthWebService (jQuery) | HTTP | Yes | 6.1 | Network | Low |

| CVE# | Component | Package and/or Privilege Required | Protocol | Remote Exploit without Auth.? | CVSS VERSION | | |
|----------------------|----------------------------|-----------------------------------|----------|-------------------------------|--------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2017-5715 | MICROS PC Workstation 2015 | BIOS | None | No | 5.6 | Local | High |

Oracle Fusion Middleware Risk Matrix

This Critical Patch Update contains 65 new security fixes for Oracle Fusion Middleware. 56 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

Oracle Fusion Middleware products include Oracle Database components that are affected by the vulnerabilities listed in the Oracle Database section. The exposure of Oracle Fusion Middleware products is dependent on the Oracle Database version being used. Oracle Database security fixes are not listed in the Oracle Fusion Middleware risk matrix. However, since vulnerabilities affecting Oracle Database versions may affect Oracle Fusion Middleware products, Oracle recommends that customers apply the October 2018 Critical Patch Update to the Oracle Database components of Oracle Fusion Middleware products. For information on what patches need to be applied to your environments, refer to Critical Patch Update October 2018 Patch Availability Document for Oracle Products, [My Oracle Support Note 24334771](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION | | |
|----------------------|---------------------------------------|--------------------------------------|----------|-------------------------------|--------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2017-5645 | BI Publisher (formerly XML Publisher) | BI Publisher Security (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2017-5645 | Oracle API Gateway | Oracle API Gateway (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-1275 | Oracle Big Data Discovery | Data Processing (Spring Framework) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-1275 | Oracle GoldenGate | Other issues (Spring | HTTP | Yes | 9.8 | Network | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION | | |
|-----------------------|--|---|----------|-------------------------------|--------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| | for Big Data | Framework) | | | | | |
| CVE-2017-5645 | Oracle Identity Analytics | Security (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2017-5645 | Oracle Identity Management Suite | Suite Level Patch Issues (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2017-15095 | Oracle Identity Manager | Installer (jackson-databind) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-3191 | Oracle WebLogic Server | WLS Core Components | T3 | Yes | 9.8 | Network | Low |
| CVE-2018-3197 | Oracle WebLogic Server | WLS Core Components | T3 | Yes | 9.8 | Network | Low |
| CVE-2018-3201 | Oracle WebLogic Server | WLS Core Components | T3 | Yes | 9.8 | Network | Low |
| CVE-2018-3245 | Oracle WebLogic Server | WLS Core Components | T3 | Yes | 9.8 | Network | Low |
| CVE-2018-3252 | Oracle WebLogic Server | WLS Core Components | T3 | Yes | 9.8 | Network | Low |
| CVE-2018-1258 | Oracle Endeca Information Discovery Integrator | Other Issues (Spring Framework) | HTTP | No | 8.8 | Network | Low |
| CVE-2018-1258 | Oracle WebLogic Server | Sample apps (Spring Framework) | HTTP | No | 8.8 | Network | Low |
| CVE-2018-2911 | Oracle GlassFish Server | Java Server Faces | HTTP | Yes | 8.3 | Network | Low |
| CVE-2016-1182 | Oracle Adaptive | OAAM Server (Apache Struts | HTTP | Yes | 8.2 | Network | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION | | |
|-------------------------|---|--|----------|-------------------------------|--------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| | Access Manager | 1) | | | | | |
| CVE-2018-3204 | Oracle Business Intelligence Enterprise Edition | Analytics Server | HTTP | Yes | 8.2 | Network | Low |
| CVE-2016-1182 | Oracle Real-Time Decision Server | Platform Installation (Apache Struts 1) | HTTP | Yes | 8.2 | Network | Low |
| CVE-2017-7805 | Oracle Directory Server Enterprise Edition | Admin Console (Sun Security Libraries) | HTTP | No | 7.5 | Network | High |
| CVE-2018-3152 | Oracle GlassFish Server | Administration | HTTP | Yes | 7.5 | Network | Low |
| CVE-2018-1000300 | Oracle HTTP Server | Web Listener (curl) | HTTP | Yes | 7.5 | Network | High |
| CVE-2018-0732 | Oracle Tuxedo | Docs-ATMI-IB (OpenSSL) | HTTPS | Yes | 7.5 | Network | Low |
| CVE-2018-3246 | Oracle WebLogic Server | WLS - Web Services | HTTP | Yes | 7.5 | Network | Low |
| CVE-2018-3213 | Oracle WebLogic Server | Docker Images | T3 | Yes | 7.5 | Network | Low |
| CVE-2018-8013 | Oracle Business Intelligence Enterprise Edition | Oracle Business Intelligence Enterprise Edition (Apache Batik) | HTTP | Yes | 7.3 | Network | Low |
| CVE-2018-8013 | Oracle Enterprise Repository | Security Subsystem - 12c (Apache Batik) | HTTP | Yes | 7.3 | Network | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION | | |
|----------------------|------------------------------|--------------------|----------|-------------------------------|--------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2018-3179 | Oracle Identity Manager | Advanced Console | HTTP | Yes | 7.2 | Network | Low |
| CVE-2018-3168 | Oracle Identity Analytics | Core Components | HTTP | No | 7.1 | Network | Low |
| CVE-2018-3217 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3218 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3219 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3220 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3221 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3302 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3222 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3223 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3224 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3225 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3226 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION | | |
|-----------------------|------------------------------|---------------------------------|----------|-------------------------------|--------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2018-3227 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3228 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3229 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3230 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3231 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3232 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3233 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3234 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-18223 | Oracle Outside In Technology | Outside In Filters (ODA Module) | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-18224 | Oracle Outside In Technology | Outside In Filters (ODA Module) | HTTP | Yes | 7.1 | Network | Low |
| CVE-2018-3238 | Oracle WebCenter Sites | Advanced UI | HTTP | No | 6.9 | Network | Low |
| CVE-2018-0739 | Oracle Endeca Server | Product Code (OpenSSL) | HTTP | Yes | 6.5 | Network | Low |
| CVE-2018-1305 | Oracle WebCenter Sites | Advanced UI (Apache Tomcat) | HTTP | No | 6.5 | Network | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION | | |
|-----------------------|--|---------------------------------|----------|-------------------------------|--------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2018-3249 | Oracle WebLogic Server | WLS - Web Services | HTTP | No | 6.5 | Network | Low |
| CVE-2018-3248 | Oracle WebLogic Server | WLS - Web Services | HTTP | Yes | 6.5 | Network | Low |
| CVE-2015-9251 | Oracle Endeca Information Discovery Studio | Studio (jQuery) | HTTP | Yes | 6.1 | Network | Low |
| CVE-2017-14735 | Oracle Fusion Middleware MapViewer | Install (AntiSamy) | HTTP | Yes | 6.1 | Network | Low |
| CVE-2015-9251 | Oracle Service Bus | OSB Core Functionality (jQuery) | HTTP | Yes | 6.1 | Network | Low |
| CVE-2015-9251 | Oracle WebCenter Sites | Advanced UI (jQuery) | HTTP | Yes | 6.1 | Network | Low |
| CVE-2018-3250 | Oracle WebLogic Server | WLS - Web Services | HTTP | Yes | 6.1 | Network | Low |
| CVE-2018-3215 | Oracle Endeca Information Discovery Integrator | Integrator ETL | HTTP | Yes | 5.4 | Network | Low |
| CVE-2018-3210 | Oracle GlassFish Server | Java Server Faces | HTTP | Yes | 5.3 | Network | Low |
| CVE-2018-3254 | Oracle WebCenter Portal | WebCenter Spaces Application | HTTP | Yes | 5.3 | Network | Low |
| CVE-2018-3253 | Oracle Virtual Directory | Virtual Directory Manager | HTTP | No | 8.5 | Network | High |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION | | |
|----------------------|------------------------------|--------------------|----------|-------------------------------|--------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2018-3147 | Oracle Outside In Technology | Outside In Filters | HTTP | Yes | 4.3 | Network | Low |
| CVE-2018-2902 | Oracle WebLogic Server | Console | HTTP | No | 4.3 | Network | Low |

Notes:

1. Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower.

Additional CVEs addressed are below:

- The fix for CVE-2016-1182 also addresses CVE-2014-0114 and CVE-2016-1181.
- The fix for CVE-2017-15095 also addresses CVE-2017-7525 and CVE-2018-7489.
- The fix for CVE-2018-0732 also addresses CVE-2018-0737.
- The fix for CVE-2018-0739 also addresses CVE-2017-3738 and CVE-2018-0733.
- The fix for CVE-2018-1000300 also addresses CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122 and CVE-2018-1000301.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The fix for CVE-2018-1275 also addresses CVE-2016-0635, CVE-2018-1258, CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.
- The fix for CVE-2018-1305 also addresses CVE-2018-1304.

Oracle Health Sciences Applications Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Health Sciences Applications. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RIS | | | |
|----------------------|--|--------------------------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2015-9251 | Oracle Healthcare Translational Research | Cohort Explorer (jQuery) | HTTP | Yes | 6.1 | Network | Low | None |

Oracle Hospitality Applications Risk Matrix

This Critical Patch Update contains 9 new security fixes for Oracle Hospitality Applications. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 F | | | |
|----------------------|--|---------------------------|----------|-------------------------------|--------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs Req'd |
| CVE-2018-1258 | Oracle Hospitality Guest Access | Base (Spring Framework) | HTTP | No | 8.8 | Network | Low | Low |
| CVE-2018-3160 | Oracle Hospitality Cruise Shipboard Property Management System | OHC Admin, OHC Management | None | No | 7.7 | Local | Low | High |
| CVE-2018-3158 | Oracle Hospitality Cruise Fleet Management | Emergency Response System | HTTP | No | 7.1 | Network | Low | Low |
| CVE-2018-3163 | Oracle Hospitality Cruise Fleet Management | Emergency Response System | HTTP | Yes | 6.5 | Network | Low | None |
| CVE-2018-3166 | Oracle Hospitality Cruise Fleet Management | Emergency Response System | HTTP | No | 6.5 | Network | Low | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 F | | | |
|----------------------|--|----------------------|----------|-------------------------------|--------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs Req'd |
| CVE-2018-1305 | Oracle Hospitality Guest Access | Base (Apache Tomcat) | HTTP | No | 6.5 | Network | Low | Low |
| CVE-2018-3159 | Oracle Hospitality Cruise Fleet Management | Sender and Receiver | None | No | 6.1 | Local | Low | Low |
| CVE-2015-9251 | Oracle Hospitality Guest Access | Base (jQuery) | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3181 | Oracle Hospitality Cruise Shipboard Property Management System | OHC ENOAD | None | No | 5.5 | Local | Low | Low |

Additional CVEs addressed are below:

- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The fix for CVE-2018-1305 also addresses CVE-2018-1304.

Oracle Hyperion Risk Matrix

This Critical Patch Update contains 9 new security fixes for Oracle Hyperion. 6 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|----------------------|---------------------------------------|---------------------|----------|-------------------------------|------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs Req'd |
| CVE-2018-3208 | Hyperion Data Relationship Management | Access and Security | HTTP | No | 7.7 | Network | Low | Low |
| CVE-2018-3142 | Hyperion Essbase | EAS Console | HTTP | No | 7.7 | Network | Low | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|----------------------|--|---------------------------|----------|-------------------------------|------------------|---------------|----------------|------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Priv: Req' |
| | Administration Services | | | | | | | |
| CVE-2018-3175 | Hyperion Common Events | User Interface | HTTP | Yes | 6.1 | Network | Low | Non |
| CVE-2018-3176 | Hyperion Common Events | User Interface | HTTP | Yes | 6.1 | Network | Low | Non |
| CVE-2018-3177 | Hyperion Common Events | User Interface | HTTP | Yes | 6.1 | Network | Low | Non |
| CVE-2018-3178 | Hyperion Common Events | User Interface | HTTP | Yes | 6.1 | Network | Low | Non |
| CVE-2018-3140 | Hyperion Essbase Administration Services | EAS Console | HTTP | Yes | 6.1 | Network | Low | Non |
| CVE-2018-3141 | Hyperion Essbase Administration Services | EAS Console | HTTP | Yes | 5.8 | Network | Low | Non |
| CVE-2018-3184 | Hyperion BI+ | IQR - Foundation Services | HTTP | No | 2.4 | Network | Low | Higl |

Oracle iLearning Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle iLearning. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RIS | | | |
|----------------------|------------------|------------------------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-3146 | Oracle iLearning | Learner Administration | HTTP | Yes | 8.2 | Network | Low | None |

Oracle Insurance Applications Risk Matrix

This Critical Patch Update contains 5 new security fixes for Oracle Insurance Applications. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK | | | |
|----------------------|-------------------------------------|---------------------------------------|----------|-------------------------------|-----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2017-5645 | Oracle Insurance Calculation Engine | Calculation engine (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low | None |
| CVE-2018-1275 | Oracle Insurance Calculation Engine | Calculation engine (Spring Framework) | HTTP | Yes | 9.8 | Network | Low | None |
| CVE-2017-5645 | Oracle Insurance Rules Palette | Rules Palette (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low | None |
| CVE-2018-1275 | Oracle Insurance Rules Palette | Rules Palette (Spring Framework) | HTTP | Yes | 9.8 | Network | Low | None |
| CVE-2018-8013 | Oracle Insurance Calculation Engine | Architecture (Apache Batik) | HTTP | Yes | 7.3 | Network | Low | None |

Additional CVEs addressed are below:

- The fix for CVE-2018-1275 also addresses CVE-2018-1270.

Oracle Java SE Risk Matrix

This Critical Patch Update contains 12 new security fixes for Oracle Java SE. 11 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

The CVSS scores below assume that a user running a Java applet or Java Web Start application (in Java SE 8) has administrator privileges (typical on Windows). When the user does not run with administrator privileges (typical on Solaris and Linux), the corresponding CVSS impact

scores for Confidentiality, Integrity, and Availability are "Low" instead of "High", lowering the CVSS Base Score. For example, a Base Score of 9.6 becomes 7.1.

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 R | | | |
|----------------------|------------------------------------|----------------|----------|-------------------------------|--------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-3183 | Java SE, Java SE Embedded, JRockit | Scripting | Multiple | Yes | 9.0 | Network | High | None |
| CVE-2018-3209 | Java SE | JavaFX | Multiple | Yes | 8.3 | Network | High | None |
| CVE-2018-3169 | Java SE, Java SE Embedded | Hotspot | Multiple | Yes | 8.3 | Network | High | None |
| CVE-2018-3149 | Java SE, Java SE Embedded, JRockit | JNDI | Multiple | Yes | 8.3 | Network | High | None |
| CVE-2018-3211 | Java SE, Java SE Embedded | Serviceability | None | No | 6.6 | Local | Low | Low |
| CVE-2018-3180 | Java SE, Java SE Embedded, JRockit | JSSE | SSL/TLS | Yes | 5.6 | Network | High | None |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 R | | | |
|-----------------------|------------------------------------|---------------------|----------|-------------------------------|--------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-3214 | Java SE, Java SE Embedded, JRockit | Sound | Multiple | Yes | 5.3 | Network | Low | None |
| CVE-2018-3157 | Java SE | Sound | Multiple | Yes | 3.7 | Network | High | None |
| CVE-2018-3150 | Java SE | Utility | Multiple | Yes | 3.7 | Network | High | None |
| CVE-2018-13785 | Java SE, Java SE Embedded | Deployment (libpng) | HTTP | Yes | 3.7 | Network | High | None |
| CVE-2018-3136 | Java SE, Java SE Embedded | Security | Multiple | Yes | 3.4 | Network | High | None |
| CVE-2018-3139 | Java SE, Java SE Embedded | Networking | Multiple | Yes | 3.1 | Network | High | None |

Notes:

1. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs.

2. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

3. This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). This vulnerability can only be exploited when Java Usage Tracker functionality is being used.

4. This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator).

Additional CVEs addressed are below:

- The fix for CVE-2018-13785 also addresses CVE-2018-14048.

Oracle JD Edwards Products Risk Matrix

This Critical Patch Update contains 6 new security fixes for Oracle JD Edwards Products. All of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 | | | |
|----------------------|---------------------------------------|--|----------|-------------------------------|------------------|---------------|----------------|-------|
| | | | | | Base Score | Attack Vector | Attack Complex | Pr Re |
| CVE-2018-7489 | JD Edwards EnterpriseOne Orchestrator | IoT Orchestrator Security (jackson-databind) | HTTP | Yes | 9.8 | Network | Low | N |
| CVE-2018-7489 | JD Edwards EnterpriseOne Tools | EnterpriseOne Mobility (jackson-databind) | HTTP | Yes | 9.8 | Network | Low | N |
| CVE-2018-7489 | JD Edwards EnterpriseOne Tools | Web Runtime (jackson-databind) | HTTP | Yes | 9.8 | Network | Low | N |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|-----------------------|--------------------------------|---|----------|-------------------------------|------------------|---------------|----------------|----|
| | | | | | Base Score | Attack Vector | Attack Complex | Pr |
| CVE-2017-15095 | JD Edwards EnterpriseOne Tools | Business Logic Inf (jackson-databind) | HTTP | Yes | 8.1 | Network | High | N |
| CVE-2017-15095 | JD Edwards EnterpriseOne Tools | Monitoring and Diagnostics (jackson-databind) | HTTP | Yes | 8.1 | Network | High | N |
| CVE-2018-0739 | JD Edwards EnterpriseOne Tools | Enterprise Infrastructure (OpenSSL) | JDENET | Yes | 6.5 | Network | Low | N |

Additional CVEs addressed are below:

- The fix for CVE-2017-15095 also addresses CVE-2017-7525.
- The fix for CVE-2018-0739 also addresses CVE-2017-3738 and CVE-2018-0733.
- The fix for CVE-2018-7489 also addresses CVE-2017-15095 and CVE-2017-7525.

Oracle MySQL Risk Matrix

This Critical Patch Update contains 38 new security fixes for Oracle MySQL. 3 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RIS | | | |
|-----------------------|--------------------------|---------------------------------------|----------|-------------------------------|----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-11776 | MySQL Enterprise Monitor | Monitoring: General (Apache Struts 2) | HTTP | Yes | 9.8 | Network | Low | None |
| CVE-2018-8014 | MySQL Enterprise Monitor | Monitoring: General (Apache Tomcat) | HTTP | Yes | 9.8 | Network | Low | None |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RIS | | | |
|----------------------|--------------------------|--|----------------|-------------------------------|----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| | | | | | | | | |
| CVE-2018-3258 | MySQL Connectors | Connector/J | X Protocol | No | 8.8 | Network | Low | Low |
| CVE-2018-1258 | MySQL Enterprise Monitor | Monitoring: General (Spring Framework) | HTTP | No | 8.8 | Network | Low | Low |
| CVE-2016-9843 | MySQL Server | InnoDB (zlib) | MySQL Protocol | No | 8.8 | Network | Low | Low |
| CVE-2018-3155 | MySQL Server | Server: Parser | MySQL Protocol | No | 7.7 | Network | Low | Low |
| CVE-2018-3143 | MySQL Server | InnoDB | MySQL Protocol | No | 6.5 | Network | Low | Low |
| CVE-2018-3156 | MySQL Server | InnoDB | MySQL Protocol | No | 6.5 | Network | Low | Low |
| CVE-2018-3251 | MySQL Server | InnoDB | MySQL Protocol | No | 6.5 | Network | Low | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RIS | | | |
|----------------------|--------------|-------------------------|----------------|-------------------------------|----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-3182 | MySQL Server | Server: DML | MySQL Protocol | No | 6.5 | Network | Low | Low |
| CVE-2018-3137 | MySQL Server | Server: Optimizer | MySQL Protocol | No | 6.5 | Network | Low | Low |
| CVE-2018-3203 | MySQL Server | Server: Optimizer | MySQL Protocol | No | 6.5 | Network | Low | Low |
| CVE-2018-3133 | MySQL Server | Server: Parser | MySQL Protocol | No | 6.5 | Network | Low | Low |
| CVE-2018-3145 | MySQL Server | Server: Parser | MySQL Protocol | No | 6.5 | Network | Low | Low |
| CVE-2018-3144 | MySQL Server | Server: Security: Audit | MySQL Protocol | Yes | 5.9 | Network | High | None |
| CVE-2018-3185 | MySQL Server | InnoDB | MySQL Protocol | No | 5.5 | Network | Low | High |
| CVE-2018-3195 | MySQL Server | Server: DDL | MySQL Protocol | No | 5.5 | Network | Low | High |
| CVE-2018-3247 | MySQL Server | Server: Merge | MySQL Protocol | No | 5.5 | Network | Low | High |
| CVE-2018-3187 | MySQL Server | Server: Optimizer | MySQL Protocol | No | 5.5 | Network | Low | High |
| CVE-2018-3174 | MySQL Server | Client programs | MySQL Protocol | No | 5.3 | Local | High | High |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RIS | | | |
|----------------------|--------------|----------------------------|----------------|-------------------------------|----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| | | | | | | | | |
| CVE-2018-3171 | MySQL Server | Server: Partition | MySQL Protocol | No | 5.0 | Network | High | High |
| CVE-2018-3277 | MySQL Server | InnoDB | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3162 | MySQL Server | InnoDB | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3173 | MySQL Server | InnoDB | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3200 | MySQL Server | InnoDB | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3170 | MySQL Server | Server: DDL | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3212 | MySQL Server | Server: Information Schema | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3280 | MySQL Server | Server: JSON | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3276 | MySQL Server | Server: Memcached | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3186 | MySQL Server | Server: Optimizer | MySQL Protocol | No | 4.9 | Network | Low | High |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RIS | | | |
|----------------------|--------------|------------------------------|----------------|-------------------------------|----------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-3161 | MySQL Server | Server: Partition | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3278 | MySQL Server | Server: RBR | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3279 | MySQL Server | Server: Security: Roles | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3282 | MySQL Server | Server: Storage Engines | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3285 | MySQL Server | Server: Windows | MySQL Protocol | No | 4.9 | Network | Low | High |
| CVE-2018-3284 | MySQL Server | InnoDB | MySQL Protocol | No | 4.4 | Network | High | High |
| CVE-2018-3283 | MySQL Server | Server: Logging | MySQL Protocol | No | 4.4 | Network | High | High |
| CVE-2018-3286 | MySQL Server | Server: Security: Privileges | MySQL Protocol | No | 4.3 | Network | Low | Low |

Additional CVEs addressed are below:

- The fix for CVE-2016-9843 also addresses CVE-2016-9840, CVE-2016-9841 and CVE-2016-9842.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.

- The fix for CVE-2018-8014 also addresses CVE-2018-1304, CVE-2018-1305, CVE-2018-8034 and CVE-2018-8037.

Oracle PeopleSoft Products Risk Matrix

This Critical Patch Update contains 24 new security fixes for Oracle PeopleSoft Products. 21 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RI | | | |
|----------------------|-----------------------------------|-------------------------------------|----------|-------------------------------|---------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2017-9798 | PeopleSoft Enterprise PeopleTools | PeopleSoft CDA (Apache HTTP Server) | HTTP | Yes | 7.5 | Network | Low | None |
| CVE-2018-3192 | PeopleSoft Enterprise PeopleTools | Query | HTTP | No | 7.2 | Network | Low | High |
| CVE-2018-3165 | PeopleSoft Enterprise PeopleTools | SQR | HTTP | No | 7.2 | Network | Low | High |
| CVE-2018-0739 | PeopleSoft Enterprise PeopleTools | Security (OpenSSL) | HTTPS | Yes | 6.5 | Network | Low | None |
| CVE-2018-3193 | PeopleSoft Enterprise PeopleTools | Activity Guide | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3194 | PeopleSoft Enterprise PeopleTools | Activity Guide | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3164 | PeopleSoft Enterprise PeopleTools | Elastic Search | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3255 | PeopleSoft Enterprise PeopleTools | Fluid Core | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3301 | PeopleSoft Enterprise PeopleTools | PIA Core Technology | HTTP | Yes | 6.1 | Network | Low | None |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RI | | | |
|----------------------|---------------------------------------|---------------------|----------|-------------------------------|---------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-3153 | PeopleSoft Enterprise PeopleTools | PIA Core Technology | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3257 | PeopleSoft Enterprise PeopleTools | PIA Core Technology | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3154 | PeopleSoft Enterprise PeopleTools | Portal | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3206 | PeopleSoft Enterprise PeopleTools | Portal | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3207 | PeopleSoft Enterprise PeopleTools | Portal | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3132 | PeopleSoft Enterprise PeopleTools | Rich Text Editor | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3205 | PeopleSoft Enterprise PeopleTools | Workflow | HTTP | Yes | 6.1 | Network | Low | None |
| CVE-2018-3130 | PeopleSoft Enterprise Interaction Hub | Application Portal | HTTP | No | 5.4 | Network | Low | Low |
| CVE-2018-3239 | PeopleSoft Enterprise PeopleTools | Integration Broker | HTTP | Yes | 5.3 | Network | Low | None |
| CVE-2018-3261 | PeopleSoft Enterprise PeopleTools | Integration Broker | HTTP | Yes | 5.3 | Network | Low | None |
| CVE-2018-3202 | PeopleSoft Enterprise PeopleTools | Performance Monitor | HTTP | Yes | 5.3 | Network | Low | None |
| CVE-2018-3198 | PeopleSoft Enterprise PeopleTools | Portal | HTTP | Yes | 5.3 | Network | Low | None |
| CVE-2018-3135 | PeopleSoft Enterprise | Portal | HTTP | Yes | 4.7 | Network | Low | None |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RI | | | |
|----------------------|-----------------------------------|------------|----------|-------------------------------|---------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| | PeopleTools | | | | | | | |
| CVE-2018-3262 | PeopleSoft Enterprise PeopleTools | Stylesheet | HTTP | Yes | 4.7 | Network | Low | None |
| CVE-2018-3129 | PeopleSoft Enterprise PeopleTools | Portal | HTTP | Yes | 4.3 | Network | Low | None |

Additional CVEs addressed are below:

- The fix for CVE-2018-0739 also addresses CVE-2017-3738 and CVE-2018-0733.

Oracle Retail Applications Risk Matrix

This Critical Patch Update contains 31 new security fixes for Oracle Retail Applications. 21 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RI | | |
|-------------------------|---|--------------------------------------|----------|-------------------------------|---------------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2016-1000031 | MICROS Relate CRM Software | Web Services (Apache Commons) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-7489 | Oracle Retail Allocation | General (jackson-databind) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-7489 | Oracle Retail Assortment Planning | Application Core (jackson-databind) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2016-1000031 | Oracle Retail Customer Management and Segmentation Foundation | Internal Operations (Apache Commons) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2017-5645 | Oracle Retail Extract | Mathematical Operators | HTTP | Yes | 9.8 | Network | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 | | |
|----------------------|---|--|----------|-------------------------------|------------------|---------------|-------------------|
| | | | | | Base Score | Attack Vector | Attack Complexity |
| | Transform and Load | (Apache Log4j) | | | | | |
| CVE-2018-7489 | Oracle Retail Invoice Matching | Security (jackson-databind) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2017-5645 | Oracle Retail Open Commerce Platform | Framework (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2017-5533 | Oracle Retail Open Commerce Platform | Framework (JasperReports) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-1275 | Oracle Retail Open Commerce Platform | Framework (Spring Framework) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2017-5533 | Oracle Retail Order Broker | Order Broker Foundation (JasperReports) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-1275 | Oracle Retail Order Broker | System Administration (Spring Framework) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-1275 | Oracle Retail Predictive Application Server | RPAS Fusion Client (Spring Framework) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-7489 | Oracle Retail Sales Audit | Operational Insights (jackson-databind) | HTTP | Yes | 9.8 | Network | Low |
| CVE-2018-1258 | MICROS Lucas | Security (Spring Framework) | HTTP | No | 8.8 | Network | Low |
| CVE-2018-1258 | Oracle Retail Assortment Planning | Application Core (Spring Framework) | HTTP | No | 8.8 | Network | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.1 | | |
|-----------------------|---------------------------------------|--|----------|-------------------------------|------------------|---------------|-------------------|
| | | | | | Base Score | Attack Vector | Attack Complexity |
| CVE-2018-1258 | Oracle Retail Financial Integration | PeopleSoft Integration Bugs (Spring Framework) | HTTP | No | 8.8 | Network | Low |
| CVE-2018-1258 | Oracle Retail Integration Bus | RIB Kernel (Spring Framework) | HTTP | No | 8.8 | Network | Low |
| CVE-2017-15095 | Oracle Retail Open Commerce Platform | Framework (jackson-databind) | HTTP | Yes | 8.1 | Network | High |
| CVE-2018-3115 | Oracle Retail Sales Audit | Operational Insights | HTTP | No | 7.7 | Network | High |
| CVE-2018-2889 | MICROS Retail-J | Internal Operations | HTTP | Yes | 7.5 | Network | Low |
| CVE-2018-8013 | Oracle Retail Back Office | Security (Apache Batik) | HTTP | Yes | 7.3 | Network | Low |
| CVE-2018-8013 | Oracle Retail Central Office | Security (Apache Batik) | HTTP | Yes | 7.3 | Network | Low |
| CVE-2018-8013 | Oracle Retail Order Broker | Upgrade Install (Apache Batik) | HTTP | Yes | 7.3 | Network | Low |
| CVE-2018-8013 | Oracle Retail Point-of-Service | Security (Apache Batik) | HTTP | Yes | 7.3 | Network | Low |
| CVE-2018-8013 | Oracle Retail Returns Management | Security (Apache Batik) | HTTP | Yes | 7.3 | Network | Low |
| CVE-2018-3122 | Oracle Retail Open Commerce Platform | Integrations | HTTP | No | 6.8 | Network | High |
| CVE-2018-3126 | Oracle Retail Xstore Point of Service | Xenvironment | HTTP | No | 6.6 | Network | High |
| CVE-2018-7489 | Oracle Retail Xstore Point of Service | Xenvironment (jackson-databind) | HTTP | No | 6.6 | Network | High |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | |
|----------------------|----------------------------|---------------------------------|----------|-------------------------------|------------------|---------------|----------------|
| | | | | | Base Score | Attack Vector | Attack Complex |
| CVE-2018-2887 | MICROS Retail-J | Back Office | HTTP | Yes | 6.5 | Network | Low |
| CVE-2018-1305 | MICROS XBRi | Retail (Apache Tomcat) | HTTP | No | 6.5 | Network | Low |
| CVE-2018-1305 | Oracle Retail Order Broker | Upgrade Install (Apache Tomcat) | HTTP | No | 6.5 | Network | Low |

Additional CVEs addressed are below:

- The fix for CVE-2017-5533 also addresses CVE-2017-5529.
- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The fix for CVE-2018-1275 also addresses CVE-2017-5529, CVE-2018-1258, CVE-2018-1270, CVE-2018-1271 and CVE-2018-1272.
- The fix for CVE-2018-1305 also addresses CVE-2018-1304.
- The fix for CVE-2018-7489 also addresses CVE-2017-7525, CVE-2018-11307 and CVE-2018-12022.

Oracle Siebel CRM Risk Matrix

This Critical Patch Update contains 3 new security fixes for Oracle Siebel CRM. 2 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|----------------------|-------------------------|------------------------------------|----------|-------------------------------|------------------|---------------|----------------|----------|
| | | | | | Base Score | Attack Vector | Attack Complex | Priv Req |
| CVE-2017-5645 | Siebel UI Framework | EAI (Apache Log4j) | HTTP | Yes | 9.8 | Network | Low | Nor |
| CVE-2018-1305 | Siebel Apps - Marketing | Mktg/Campaign Mgmt (Apache Tomcat) | HTTP | No | 6.5 | Network | Low | Low |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|----------------------|---------------------|-------------|----------|-------------------------------|------------------|---------------|----------------|----------|
| | | | | | Base Score | Attack Vector | Attack Complex | Priv Req |
| CVE-2018-3059 | Siebel UI Framework | UIF Open UI | HTTP | Yes | 6.1 | Network | Low | Nor |

Additional CVEs addressed are below:

- The fix for CVE-2018-1305 also addresses CVE-2018-1304.

Oracle Sun Systems Products Suite Risk Matrix

This Critical Patch Update contains 19 new security fixes for the Oracle Sun Systems Products Suite. 9 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RI | | | |
|----------------------|--|------------------------------------|----------|-------------------------------|---------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2016-7167 | Fujitsu M10-1, M10-4, M10-4S, M12-1, M12-2, M12-2S Servers | XCP Firmware (curl) | Multiple | Yes | 9.8 | Network | Low | None |
| CVE-2016-7167 | SPARC Enterprise M3000, M4000, M5000, M8000, M9000 Servers | XCP Firmware (curl) | Multiple | Yes | 9.8 | Network | Low | None |
| CVE-2018-3273 | Solaris | Remote Administration Daemon (RAD) | Multiple | Yes | 8.1 | Network | Low | None |
| CVE-2016-5244 | Solaris | Kernel | Multiple | Yes | 7.5 | Network | Low | None |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RI | | | |
|----------------------|---------|-------------------------------------|------------|-------------------------------|---------------------|---------------|----------------|-------------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd |
| CVE-2018-3275 | Solaris | LibKMIP | Multiple | Yes | 7.4 | Network | High | None |
| CVE-2018-3272 | Solaris | Kernel Zones Virtualized NIC Driver | None | No | 6.2 | Local | Low | None |
| CVE-2018-3274 | Solaris | Kernel | SMB | No | 5.7 | Network | Low | Low |
| CVE-2018-3263 | Solaris | Sudo | Multiple | Yes | 5.6 | Network | High | None |
| CVE-2015-6937 | Solaris | Kernel | None | No | 5.5 | Local | Low | Low |
| CVE-2018-3267 | Solaris | LFTP | FTP | Yes | 5.3 | Network | Low | None |
| CVE-2018-3271 | Solaris | Kernel Zones | None | No | 5.3 | Local | High | High |
| CVE-2018-3172 | Solaris | RPC | Portmap v3 | Yes | 5.3 | Network | Low | None |
| CVE-2018-3268 | Solaris | SMB Server | SMB | Yes | 5.3 | Network | Low | None |
| CVE-2018-3265 | Solaris | Zones | None | No | 4.9 | Local | High | None |
| CVE-2018-3264 | Solaris | Kernel | None | No | 4.4 | Local | Low | Low |
| CVE-2018-3269 | Solaris | SMB Server | SMB | No | 4.3 | Network | Low | Low |
| CVE-2018-3266 | Solaris | Verified Boot | None | No | 3.9 | Local | High | High |
| CVE-2018-2922 | Solaris | Kernel | None | No | 2.5 | Local | High | Low |
| CVE-2018-3270 | Solaris | Kernel | None | No | 1.8 | Local | High | High |

Notes:

1. SPARC Enterprise M3000, M4000, M5000, M8000, M9000 Servers are not affected by CVE-2017-7407 and CVE-2016-7141.

Additional CVEs addressed are below:

- The fix for CVE-2015-6937 also addresses CVE-2015-7990.
- The fix for CVE-2016-7167 also addresses CVE-2015-3144, CVE-2015-3145, CVE-2015-3153, CVE-2015-3236, CVE-2015-3237, CVE-2016-0755, CVE-2016-3739, CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-7141, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2016-9586 and CVE-2017-7407.

Oracle Supply Chain Products Suite Risk Matrix

This Critical Patch Update contains 6 new security fixes for the Oracle Supply Chain Products Suite. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 | | | |
|----------------------|---|--|----------|-------------------------------|------------------|---------------|----------------|----------|
| | | | | | Base Score | Attack Vector | Attack Complex | Priv Req |
| CVE-2018-1258 | Oracle Agile PLM | Application Server (Spring Framework) | HTTP | No | 8.8 | Network | Low | Low |
| CVE-2018-1305 | Oracle Agile Engineering Data Management | Install (Apache Tomcat) | HTTP | No | 6.5 | Network | Low | Low |
| CVE-2018-1305 | Oracle Agile PLM | Folders, Files & Attachments (Apache Tomcat) | HTTP | No | 6.5 | Network | Low | Low |
| CVE-2018-1305 | Oracle Transportation Management | Install (Apache Tomcat) | HTTP | No | 6.5 | Network | Low | Low |
| CVE-2018-3134 | Oracle Agile Product Lifecycle Management for Process | User Group Management | None | No | 5.0 | Local | High | Low |
| CVE-2018-3127 | Oracle Demantra Demand Management | Product Security | HTTP | Yes | 4.3 | Network | Low | None |

Additional CVEs addressed are below:

- The fix for CVE-2018-1258 also addresses CVE-2018-11039, CVE-2018-11040 and CVE-2018-1257.
- The fix for CVE-2018-1305 also addresses CVE-2018-1304.

Oracle Support Tools Risk Matrix

This Critical Patch Update contains 1 new security fix for Oracle Support Tools. This vulnerability is remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK (Score) | | | | |
|----------------------|-------------------|---------------------------------|----------|-------------------------------|-------------------------------|---------------|----------------|-------------|-----------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd | User Int. |
| CVE-2018-0739 | OSS Support Tools | Services Tools Bundle (OpenSSL) | HTTP | Yes | 6.5 | Network | Low | None | Remote |

Additional CVEs addressed are below:

- The fix for CVE-2018-0739 also addresses CVE-2017-3738 and CVE-2018-0733.

Oracle Virtualization Risk Matrix

This Critical Patch Update contains 14 new security fixes for Oracle Virtualization. 1 of these vulnerabilities may be remotely exploitable without authentication, i.e., may be exploited over a network without requiring user credentials. The English text form of this Risk Matrix can be found [here](#).

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK (Score) | | | | |
|----------------------|----------------------|-----------|----------|-------------------------------|-------------------------------|---------------|----------------|-------------|-----------|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd | User Int. |
| CVE-2018-3294 | Oracle VM VirtualBox | Core | VRDP | No | 9.0 | Network | Low | Low | Remote |
| CVE-2018-3288 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | Remote |
| CVE-2018-3289 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | Remote |

| CVE# | Product | Component | Protocol | Remote Exploit without Auth.? | CVSS VERSION 3.0 RISK | | | | |
|----------------------|----------------------|----------------|----------|-------------------------------|-----------------------|---------------|----------------|-------------|---|
| | | | | | Base Score | Attack Vector | Attack Complex | Privs-Req'd | I |
| CVE-2018-3290 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-3296 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-3297 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-2909 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-3298 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-3291 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-3292 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-3293 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-3295 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-3287 | Oracle VM VirtualBox | Core | None | No | 8.6 | Local | Low | None | R |
| CVE-2018-0732 | Oracle VM VirtualBox | Core (OpenSSL) | TLS | Yes | 7.5 | Network | Low | None | |

Additional CVEs addressed are below:

- The fix for CVE-2018-0732 also addresses CVE-2018-0737.

